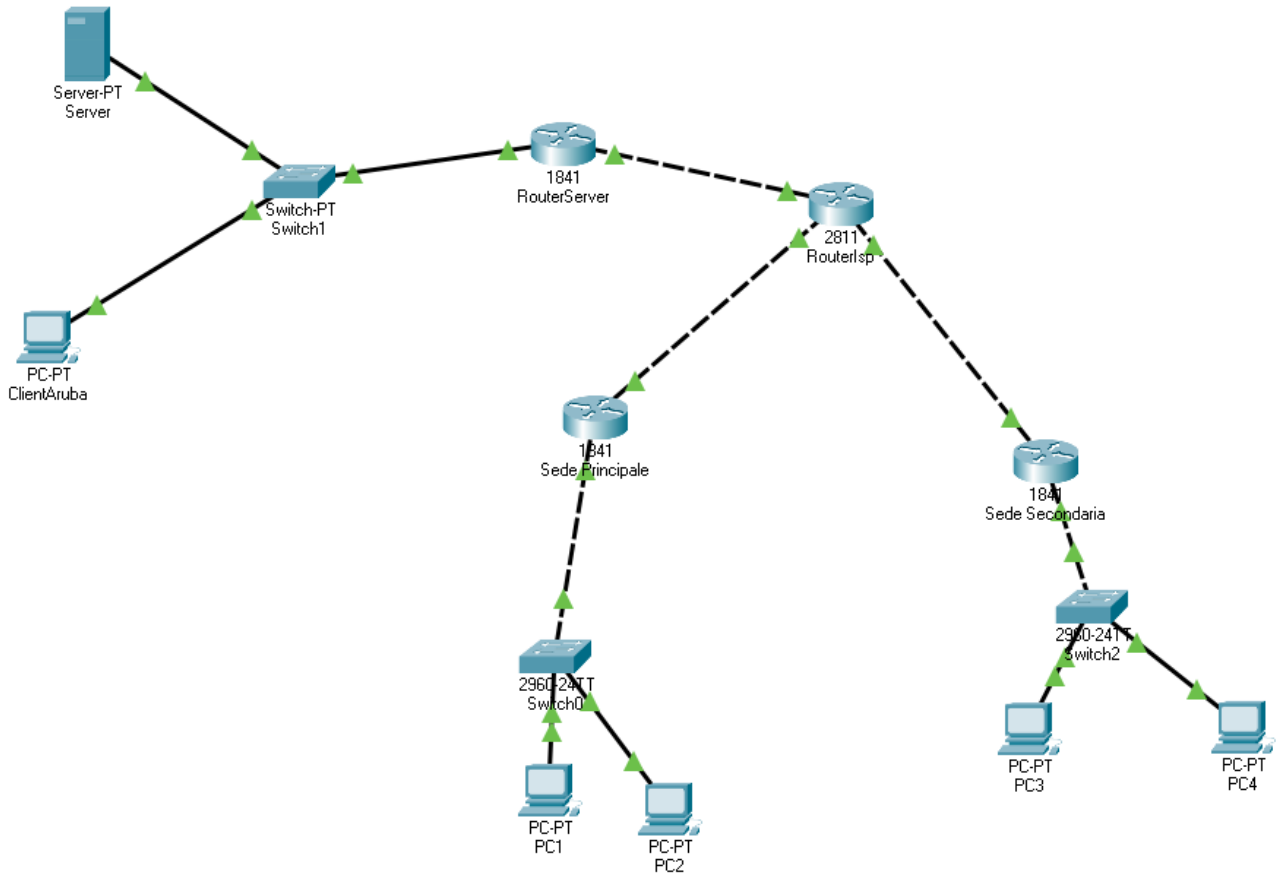
Blue Horizon S.P.A.

Organizzazione Rete

Il funzionamento della nostra rete informatica è basato su una VPN per il collegamento tra le sedi e poi usiamo la rete cellulare per poter inviare i dati raccolti dalla centralina ambientale. L'obiettivo della VPN è quello di instaurare una connessione protetta tra più sedi in modo da poter comunicare in modo sicuro i dati riguardanti i database e le prenotazioni effettuate e i dati amministrativi dislogati nelle varie sedi in tutta Italia. La rete cellulare che è stata implementata nei router 4G/3G che forniranno connessione wireless ai portatili che sono presenti all'interno delle nostre imbarcazioni consentiranno la comunicazione dei dati ambientali (quando disponibile connessione rete mobile) che comunicherà con il Database SQL predisposto nella nostra azienda, che archivia diverse tipologie di dati tra cui i dati relativi all'inquinamento ambientale, prenotazioni, contabilità, e amministrazione aziendale.

- **Progetto Rete(Schema di indirizzamento e strategia):**

Il progetto della rete è basato su una VPN Site-to-Site per il collegamento tra le sedi. Sono stati implementati due tunnel vpn (per router) che permettono l'instradamento dei pacchetti su una connessione logica per rendere la trasmissione molto più sicura della rete pubblica.



- **Gli indirizzi Ip usati nel Tunnel Vpn per la configurazione sono i seguenti:**

Nel Router dedicato alla linea dei Server abbiamo due tunnel Vpn una configurata per comunicare con la sede secondaria (Indirizzo Ip: 172.16.1.1 con Subnet mask 255.255.0.0) e l'altra per comunicare con la sede principale (Indirizzo Ip: 172.18.1.1 con Subnet mask 255.255.0.0).

Nel Router della sede principale possediamo due tunnel Vpn una configurata per comunicare con la sede dei server (Indirizzo Ip: 172.18.1.2 con Subnet mask 255.255.0.0) mentre per comunicare con la sede secondaria usiamo(Indirizzo Ip: 172.17.1.1 con Subnet mask 255.255.0.0).

Nel Router della sede secondaria abbiamo due tunnel Vpn una configurata per comunicare con la sede del server con ip (Indirizzo Ip: 172.16.1.2 con Subnet mask 255.255.0.0) e per la comunicazione con la sede principale (Indirizzo Ip: 172.18.1.2 con Subnet mask 255.255.0.0).

Mentre i comandi per effettuare la configurazione su Packet Tracer sono i seguenti:

r1#config t **(richiama la gestione della configurazione del router)**

r1(config)#interface tunnel 10 **(crea un tunnel Vpn)**

r1(config-if)#ip address 172.16.1.1 255.255.0.0 **(assegna l'indirizzo al tunnel vpn)**

r1(config-if)#tunnel source fa0/1 **(assegna al tunnel Vpn da dove provengono i pacchetti)**

r1(config-if)#tunnel destination 2.0.0.2 **(esplicita dove devono essere rinviati i pacchetti)**

Lo scopo di questi tunnel è creare una "linea sicura" che ci consentirà di far viaggiare i nostri pacchetti in modo che non vengano intercettati da chi non autorizzato. Per cui lo scopo è evitare che qualche malintenzionato possa bypassare le nostre reti.

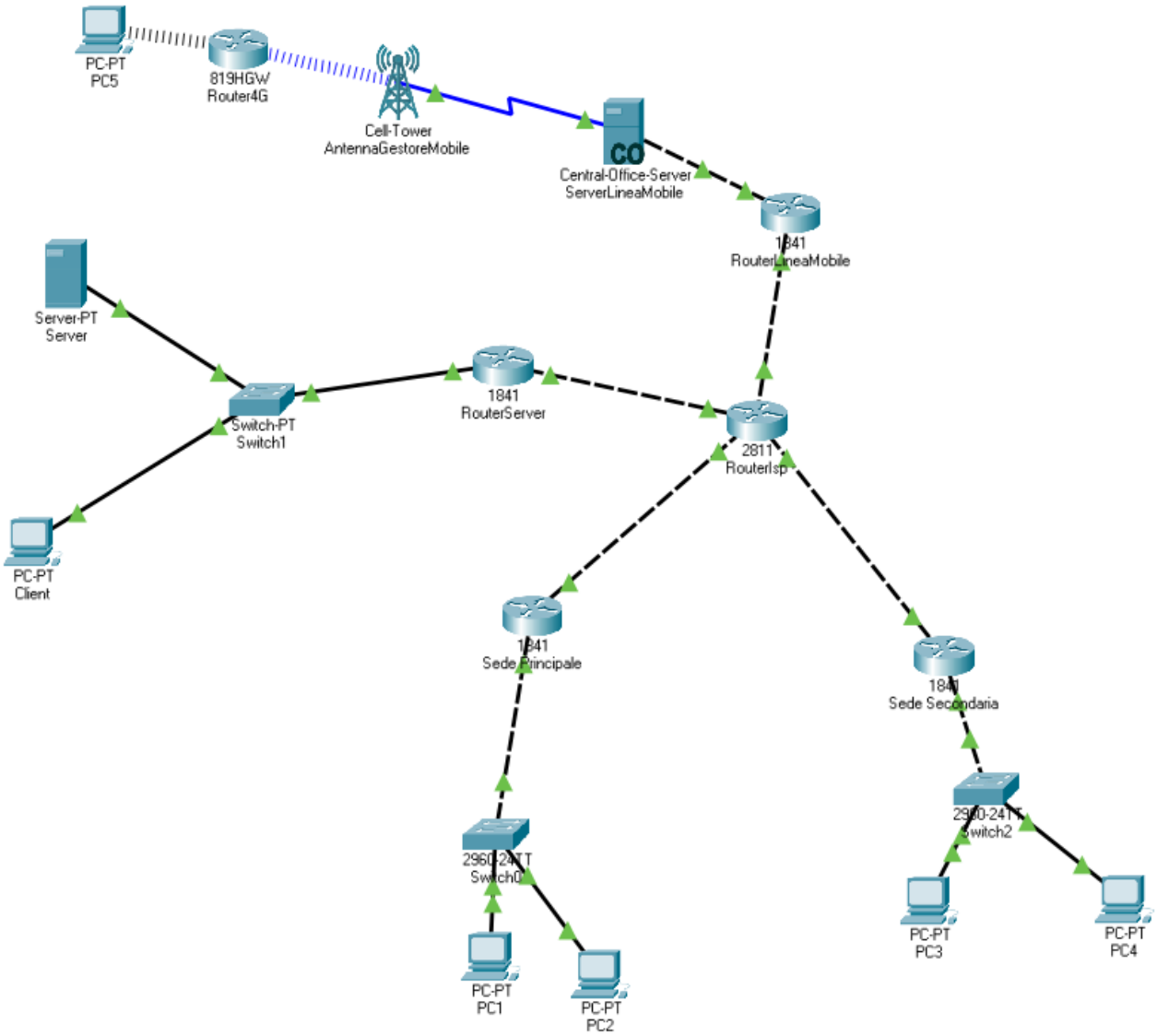
- **Gli indirizzi Ip usati nella configurazione per l'instradamento:**

il router della prima sede ha un indirizzo IP pubblico di classe A (1.0.0.1 con subnet Mask 255.0.0.0), la rete locale è basata su un indirizzo IP privato di classe C (192.168.1.1 con subnet Mask 255. 255. 255.0), l'IP default gateway è di classe C (192.168.1.1 con subnet Mask 255. 255. 255.0)

il router della seconda sede ha un indirizzo IP pubblico di classe A (2.0.0.2 con subnet Mask 255.0.0.0), la rete locale è basata su un indirizzo IP privato di classe C (192.168.2.0 con subnet Mask 255. 255. 255.0), l'IP default gateway è di classe C (192.168.2.1 con subnet Mask 255. 255. 255.0).

Il Router della sede dei Server ha un server che svolge funzioni DNS, http/s, E-mail , il server ha indirizzo (192.168.5.5 con subnet mask 255.255.255.0) ha come indirizzo pubblico (3.0.0.2 con subnet mask 255.0.0.0) e indirizzo privato (192.168.5.1 con subnet mask 255.255.255.0)

Il Router dell'Isp e basata quattro indirizzi pubblici con subnet Mask 255.0.0.0 (1.0.0.2(riservato alla sede principale),2.0.0.1(riservato alla sede secondaria),3.0.0.1(riservato alla linea dei Server Aruba),10.0.0.1(linea cellulare)



Abbiamo simulato l'infrastruttura di una rete cellulare chiamata WindTre a cui si connettono i vari pc che sono installati sulle barche, all'interno di ogni imbarcazione possediamo un router 4G/3G che fornirà connessione wireless al portatile, che potrà inviare i dati al nostro database. Il router che si connette alla Cell Tower WindTre da cui avrà assegnato un indirizzo tramite DHCP dal server della rete mobile (172.16.1.100 di classe C con subnet mask 255.255.255.0), successivamente il router 4G/3G assegnerà un indirizzo tramite DHCP(rete: 10.10.10.0 con subnet mask 255.255.255.248, in questa rete è stato applicato un subnetting per poter connettere al massimo 8 dispositivi).

- **Spiegazioni e Riflessioni Generali:**

Le nostre barche comunicano tramite i router 4G/3G predisposti all'interno delle nostre imbarcazioni che ci forniranno i dati relativi all'inquinamento, mentre il sistema AIS tramite un trasmettitore VHS andrà a trasmettere i dati a un antenna che a sua volta sarà collegata ad un computer che andrà a immagazzinare i dati sul nostro server.

Le funzionalità richieste dalla nostra azienda sono: l'hosting del sito web, database (contabilità, inquinamento, altro), email aziendali, e in più l'emissione del certificato SSL, che sono forniti da Aruba. In modo da poter ridurre i costi aziendali e la gestione dei server che è affidata a terze parti garantendo una maggiore sicurezza e affidabilità per i servizi richiesti dalla nostra azienda.

I Server Web distribuiti da Aruba sfruttano il protocolli http, e https per garantire una maggiore sicurezza a chi paga sul nostro sito perché possediamo un Certificato SSL che ci consente di poter garantire i massimi standard di sicurezza. Successivamente le nostre email sono registrate sotto dominio di @bluehorizon.it() che sfruttano i protocolli SMTP (Posta in Uscita) con porta 465 provvista di SSL e server (smtps.bluehorizon.it) e protocolli Imap(Posta in Ricezione) con porta 993(SSL) e server (imaps.bluehorizon.it). Tutti le nostre Workstation sfruttano il protocollo IMAPS per permettere ai nostri dipendenti di poter sincronizzare il loro lavoro ovunque si trovano. Ma si può anche sfruttare il protocollo POP3S(Posta in Ricezione) con porta 995 e server (pop3s.bluehorizon.it).

Per La realizzazione di una Vpn Site-To-Site viene usato OpenVpn che ci permette di creare una vpn privata tra il nostro server e i client che sono nelle nostre sedi anche per chi lavora fuori sede. Sui nostri server aziendali abbiamo un software Vpn che si collega alla nostro server , e ci consentirà l'accesso a dati come documenti e altro dati conservati nelle nostre workstation.

Tutte queste funzioni saranno gestite dai tecnici informatici che si occupano di tutta la gestione della rete, tra cui la gestione dei domini, e della configurazione dei software che servono in azienda tra cui: Il Software OpenVpn Connect installato sul server che successivamente importando il file .ovpn ed installando il seguente software anche nei client accederanno alla vpn privata e potranno connettersi anche i lavoratori che sono impegnati fuori sede o sono in smart working.